PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-244833
(43)Date of publication of application : 02.09.1994

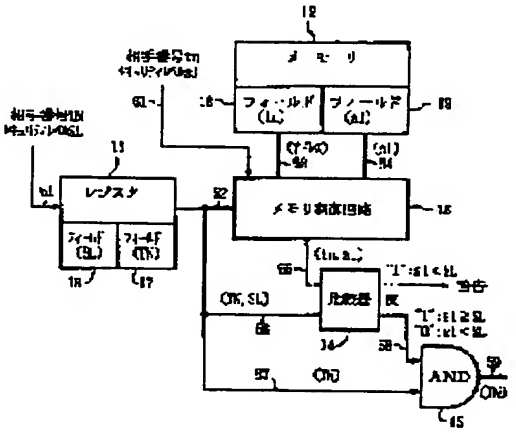
(51)Int.Cl. H04L 9/32
H04M 3/42

(21)Application number : 03-220119
(22)Date of filing : 30.08.1991

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAJIMA SEIICHI
HARADA YONOSUKE
YOSHIDA MAKOTO

(54) COMMUNICATION SECURITY SYSTEM

(57)Abstract:
PURPOSE: To prevent the communication contents from being transferred to a communication opposite party from whom the content is kept a secret by a simple method by comparing the reception security level of the communication opposite party and the information security level on a transmission side and connecting the transmission side with the only communication opposite party having the reception security level which is higher than the information security level.
CONSTITUTION: The information security level SL stored in a field 16 is inputted in a comparator 14 via a control line 56, and a reception security level sl and an information security level SL are compared. In the case of (reception security level sl) ≥ (information security level SL), the logic of a control line 58 becomes 1, the communication opposite party number TN stored in a field 17 via a control line 57 is inputted in an AND line 15 and the communication opposite party number TN is outputted to a control line 59 via the AND circuit 15.
The communication opposite party number TN outputted from the control line 59 is outputted to the central control unit, etc., of a communication network or an exchange and a communication is set.



LEGAL STATUS

[Date of request for examination] 27.08.1998
[Date of sending the examiner's decision of rejection] 20.08.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－244833

(43)公開日　平成６年(1994)９月２日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　9/32					
Ｈ０４Ｍ　3/42	Ｅ				
		7117－5K	Ｈ０４Ｌ	9/ 00	Ａ

審査請求　未請求　請求項の数１　ＯＬ　（全 ６ 頁）

(21)出願番号　特願平3－220119

(22)出願日　平成３年(1991)８月30日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　中島　誠一
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　原田　要之助
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　吉田　真
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

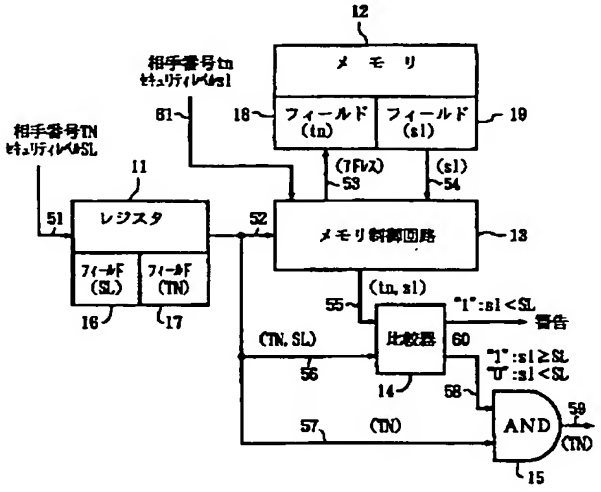
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　通信セキュリティ方式

(57)【要約】

【目的】　情報通信網において、簡単な方法により通信内容が秘密とすべき相手には転送されないようにすることが可能な通信セキュリティ方式の提供を目的とする。

【構成】　情報通信網における通信セキュリティ方式であって、予め通信相手に対応させた受信セキュリティレベルを設定して記憶しておき、通信する際に転送すべき情報に情報セキュリティレベルを設定し、通信開始時に通信相手の受信セキュリティレベルと転送すべき情報セキュリティレベルとを比較し、通信相手の受信セキュリティレベルが送信側の送信セキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないように構成する。この方式は１対１の通信時にも、多対１の通信時にも適用でき、また、通信途中で情報セキュリティレベルを変えることもできる。



【特許請求の範囲】
【請求項１】　情報通信網における通信セキュリティ方式であって、
予め通信相手に対応させた第１のセキュリティレベルを設定して記憶しておき、通信する際に転送すべき情報に第２のセキュリティレベルを設定し、通信開始時に通信相手の第１のセキュリティレベルと転送すべき情報の第２のセキュリティレベルとを比較し、通信相手の第１のセキュリティレベルが送信側の第２のセキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないことを特徴とする通信セキュリティ方式。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は通信セキュリティ方式に関し、特に、通信相手のセキュリティレベルと、転送すべき情報のセキュリティレベルに応じて、通信セキュリティを確保する通信セキュリティ方式に関するものである。
【０００２】
【従来の技術】近年、社会の情報通信システムの発達により、通信が身近になっていつでも、誰とでも通信することが可能となってきている。例えば、電話網等を利用したファクシミリ通信の普及や、パーソナルコンピュータ等を利用したデータ通信の普及により、通信者は文字情報だけでなく、図形などのイメージ情報も送受信可能である。
【０００３】しかしながら、一方では逆にこの便利さの影の部分も問題になってきている。従来の電話通信では、人間が直接介在するために、呼設定フェーズ後の通信フェーズにおいて通信相手を音声で確認してから通話を開始するため、誤ってダイヤルしても目的とする通信相手以外の第３者に通信内容が転送されることは防止できていた。ところが、ファクシミリ通信等の機械対機械の通信では、通信フェーズにおいて、通常、通信相手を確認しないため、誤ダイヤルをすると第３者に通信内容が転送されてしまうことになる。
【０００４】ファクシミリ通信ではこのような誤ダイヤルを防止ため、従来は以下のような方法がとられていた。
【０００５】１　まず、通信相手を呼出し、音声で相手を確かめてからファクシミリ通信を開始するようにする。
【０００６】２　同報通信を行う場合は、同報相手をあらかじめグループ化して誤りを防止する。
【０００７】３　ファクシミリ信号を暗号化して送信する。
【０００８】
【発明が解決しようとする課題】しかしながら、１の方法は、人手が介入するため繁雑になる問題がある。また、ファクシミリ通信では同報通信を行うことが多々あり、多数の通信相手を指定するため必然的にダイヤル誤りの確率も高くなる問題もある。また、２の方法はグループの選択を誤り他の同報グループに通信内容が転送されてしまう恐れがある。更に、３の方法は端末機のコスト上昇、伝送効率の低下、端末での暗号／復号処理による転送時間の伸長等が問題になり、また、暗号／復号の鍵管理が繁雑になる問題もある。
【０００９】本発明は上記事情に鑑みてなされたもので、その目的とするところは、簡単な方法により通信内容が秘密とすべき相手には転送されないようにすることが可能な通信セキュリティ方式を提供することにある。
【００１０】
【課題を解決するための手段】前記目的を達成する本発明は情報通信網における通信セキュリティ方式であって、予め通信相手に対応させた第１のセキュリティレベル（受信セキュリティレベル）を設定して記憶しておき、通信する際に転送すべき情報に第２のセキュリティレベル（以降、情報セキュリティレベル）を設定し、通信開始時に通信相手の受信セキュリティレベルと転送すべき情報セキュリティレベルとを比較し、通信相手の受信セキュリティレベルが送信側の送信セキュリティレベル以上の場合にのみ通信を設定し、それ以外の場合には通信を設定しないことを特徴とするものである。
【００１１】
【作用】本発明によれば、情報送信時に通信相手の受信セキュリティレベルと送信側の情報セキュリティレベルが比較され、情報セキュリティレベル以上の受信セキュリティレベルをもつ通信相手にのみ送信側が接続されるため、例えば通信相手を誤ってダイヤルしても接続されず、秘密がもれて問題となる相手に誤って情報が転送されることはなくなり、通信セキュリティを確保することができる。また、簡単な構成であるため、経済的な負担も少ない。
【００１２】
【実施例】以下、本発明の実施例を図面に基づいて詳細に説明する。図１は本発明の通信セキュリティ方式の一実施例の構成を示すものであって、１１はレジスタ、１２はメモリ、１３はメモリ制御回路、１４は比較器、１５はＡＮＤ回路、１６，１７はレジスタ１１のフィールド、１８，１９はメモリ１２のフィールド、５１，５２，５３，５４，５５，５６，５７，５８，５９，６０，６１は制御線を示している。
【００１３】通信網のユーザが通信相手番号TNとその情報セキュリティレベルSL（SL＝0，1，2 ……，Ｎで、数が大きいほどセキュリティレベルが高いことを示す）を指定すると、これらの情報は制御線５１を介してレジスタ１１に入力され、通信相手番号TNはフィールド１７に、情報セキュリティレベルSLはフィールド１６に記憶される。通信相手番号TNが制御線５２を介してメモリ制

御回路１３に入力されると、メモリ制御回路１３は制御線５３を介して番地を指定し、メモリ１２の内容を制御線５４を介して順次読み出す。フィールド１８には通信相手番号tnが、フィールド１９には受信セキュリティレベルsl（sl＝0，1，2 ……，Ｎ）が予め制御線６１を介して設定されている。

【００１４】メモリ制御回路１３は、読み出されたフィールド１８に記憶されていた通信相手番号tnとレジスタ１１から入力された通信相手番号TNを比較し、一致した場合には制御線５５にフィールド１９に記憶されたこの通信相手番号tnの受信セキュリティレベルslを出力する。なお、通信相手番号TNがフィールド１８に存在しない場合には制御線５５には最低のセキュリティレベルが出力される。フィールド１６に記憶された情報セキュリティレベルSLは制御線５６を介して比較器１４に入力され、受信セキュリティレベルslと情報セキュリティレベルSLとが比較される。

【００１５】そして、（受信セキュリティレベルsl）≧（情報セキュリティレベルSL）の場合には制御線５８はの論理は"1"になり、制御線５７を介してフィールド１７に記憶された通信相手番号TNがＡＮＤ回路１５に入力され、通信相手番号TNがＡＮＤ回路１５を介して制御線５９に出力される。制御線５９から出力された通信相手番号TNは通信網、あるいは交換機の中央制御装置等に送出されて通信が設定される。

【００１６】一方、（受信セキュリティレベルsl）＜（情報セキュリティレベルSL）の場合には、制御線５８の論理は"0"になり、制御線５９には通信相手番号は出力されず、また制御線６０の論理は"1"となる。制御線６０の論理が"1"であることは、受信セキュリティレベルsl＜情報セキュリティレベルSLであることを示し、ユーザに警告を発するものである。また、制御線５９には通信相手番号が出力されないため、通信は拒絶される。

【００１７】したがって、以上説明したように、受信セキュリティレベルが情報セキュリティレベル以上の場合にのみ通信が設定され、受信セキュリティレベルが情報セキュリティレベル未満の通信相手には通信が拒絶されるため、ユーザが転送すべき情報にセキュリティレベルを付加することにより、受信セキュリティレベルがそれ以下の相手には通信が拒絶され、セキュリティを確保することができる。

【００１８】なお、図１の機構は端末に設置することも、通信網内、例えば、交換機に設置することも可能である。更に、端末に設置される場合には、例えば、制御線５９の先は端末の選択信号送出回路等に接続され、制御線６０は警告ランプ等を起動し、また、交換機に設置された場合には、例えば、制御線５９は交換機の呼処理継続を起動し、また制御線６０は呼損処理を起動することになる。

【００１９】以上の説明では、通信相手が単数の場合であったが、１つの情報を複数の通信相手に転送する同報通信の場合においても本発明は適用できるものであり、この場合には、複数の通信相手に対応する受信セキュリティレベルについて情報セキュリティレベルとの比較を前述のように行い、（受信セキュリティレベルsl）≧（情報セキュリティレベルSL）の通信相手にのみ通信を設定し、他の通信相手の通信は拒絶するように制御すればよい。

【００２０】また、前述の説明ではファクシミリ通信を例にとって説明したが、本発明はファクシミリ通信に限定するものではなく、文書通信等の他の通信にも適用できることは明らかである。

【００２１】更に、前述の説明では、呼の設定フェーズを例にとり説明したが、本発明は通信中においても適用することができる。例えば、会議電話、テレビ会議等において、特定の会話や画面を参加者のセキュリティレベルに応じて転送の制御をする必要が生じる場合がある。このような場合、参加者間におけるセキュリティが必要な会話や画面の転送の前に、前述と同様に情報セキュリティレベルを入力し、受信セキュリティレベルが情報セキュリティレベル以上の相手にのみ情報を転送することが可能になる。

【００２２】図２はテレビ会議に本発明を適用した別の実施例を示すものであって、特定の参加者の端末装置の例を示すものである。図において、７０はメモリ、７１はレジスタ、７２はデコーダ、７３，７４はＡＮＤ回路、７５，７６はフリップフロップ（以降Ｆ／Ｆと記す）、７７，７８はＡＮＤ回路、９０は情報線、９１，９２，９３，９４，９５，９６，９７，９８，９９，１００，１０１は制御線である。また、図１と同じ構成の部材には同じ符号が付されており、１３はメモリ制御回路、１４は比較器、１８，１９はメモリ１２のフィールド、５３，５４，５５，５６，５８，６１は制御線を示している。

【００２３】なお、ＡＮＤ回路７３→Ｆ／Ｆ７５→ＡＮＤ回路７７の経路はテレビ会議への各々の参加者に対応しており、制御線９８，９９等は参加者への伝送回路に接続されている。テレビ会議の冒頭には制御線６１を介して参加者の受信セキュリティレベルslがメモリ７０に設定される。また、説明を簡単にするために参加者の番号とメモリ７０のアドレスは一致するものとする。更に、テレビ会議の冒頭には制御線１００を介して最も低い情報セキュリティレベルsmがレジスタ７１に設定され、後にセキュリティが必要になった時にその時の参加者のレベルに応じた情報セキュリティレベルSLが設定される。

【００２４】最も低い情報セキュリティレベルsmが設定されると、制御線１０１を介してメモリ制御回路１３が起動される。制御線５３にはアドレスが発生されメモリ７０に設定された参加者各々の受信セキュリティレベル

slが制御線５４を介して呼び出され、その値は制御線５５に出力される。制御線５６にはレジスタ７１に入力された情報セキュリティレベルsmまたはSLが加わり、比較器１４において、受信セキュリティレベルslと情報セキュリティレベルsmまたはSLが比較され、（受信セキュリティレベルsl）≧（情報セキュリティレベルsmまたはSL）の場合には制御線５８の論理は"1"になる。同時に制御線９１に前述のアドレスが入力され、デコーダ７２がこのアドレスをデコードし、例えば、制御線９３が選択されて論理が"1"になる。制御線９３と制御線５８の論理積がＡＮＤ回路７３でとられ、制御線９４の論理値にＦ／Ｆ７５はセットされる。

【００２５】従って、（参加者の受信セキュリティレベルsl）≧（情報セキュリティレベルsmまたはSL）の場合にはその参加者に対応するＦ／Ｆ７５等は論理が"1"に設定され、それ以外の場合にはＦ／Ｆ７５等は論理が"0"に設定される。情報線９０には会話や画像の符号化された情報が乗っており、ＡＮＤ回路７７等で論理積がとられ、Ｆ／Ｆ７５等の論理が"1"に設定された参加者のみに会話や画像情報が制御線９８等に出力されることになる。メモリ制御回路１３はすべての参加者のアドレスを発生し、Ｆ／Ｆ７５等を所定の値に設定する。

【００２６】前述のようにテレビ会議の冒頭では最も低い情報セキュリティレベルsmが設定されるため、最初はＦ／Ｆ７５，７６等はすべて論理が"1"に設定され、この端末からすべての参加者に会話や画像情報が転送されることになる。セキュリティが必要になった場合には、情報セキュリティレベルSLを制御線１００を介して再設定すると、前述のようにすべての参加者について受信セキュリティレベルslと情報セキュリティレベルSLとが比較され、ＦＦ７５等を新たな値に再設定する。したがって、（受信セキュリティレベルsl）＜（情報セキュリティレベルSL）の参加者のＦ／Ｆは論理が"0"に設定されるため、情報線９０の情報はその参加者には転送されず、セキュリティが確保される。

【００２７】情報セキュリティレベルSLを変更したいときには、任意の時点で制御線１００を介して新たな情報セキュリティレベルSLを入力することにより、任意の所要のセキュリティが確保できる。

【００２８】

【発明の効果】以上説明したように本発明によれば、情報セキュリティレベル以上の受信セキュリティレベルをもつ通信相手にのみ通信が設定されるため、例えば、通信相手を誤ってダイヤルしても秘密がもれて問題となる相手には情報が転送されず、この結果、通信セキュリティを確保することができる。また、テレビ会議のような多対１の通信における通信フェーズにおいて、各々の通信情報のセキュリティレベルに応じて特定の通信相手にのみ情報を転送する等の制御も可能となる。

【００２９】本発明では、従来の対策や方式のように人手が介入したり、端末が複雑になったり、転送時間が伸長する等の問題もなく、さらに簡単な構成であるため経済的な負担も少い特徴をもっている。

【図面の簡単な説明】

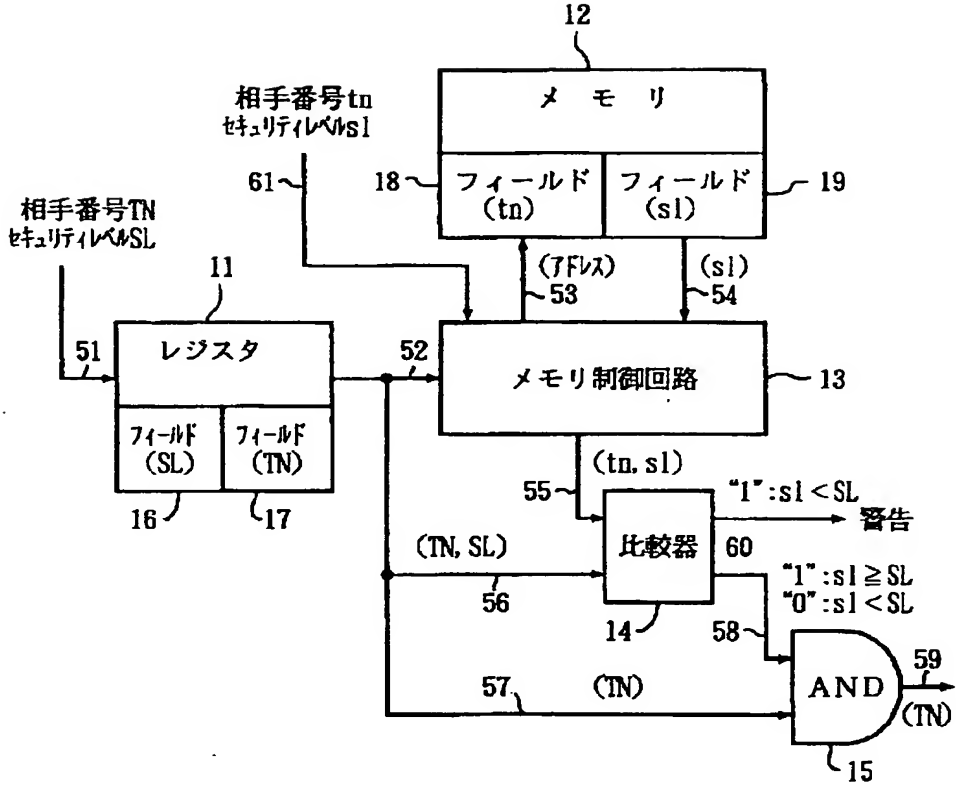
【図１】本発明の通信セキュリティ方式の一実施例を示すものである。

【図２】本発明の他の実施例を示すものである。

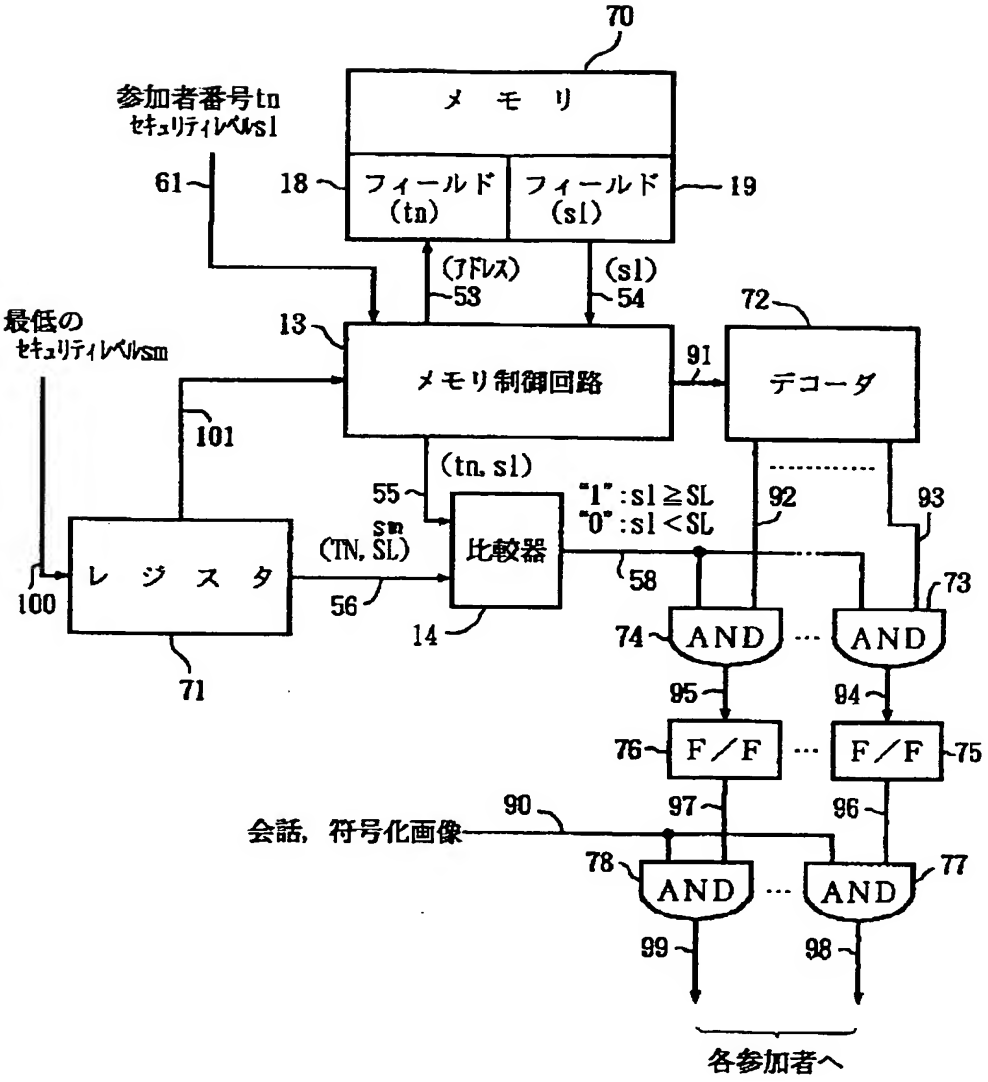
【符号の説明】

１１　レジスタ
１２　メモリ
１３　メモリ制御回路
１４　比較器
１５　ＡＮＤ回路
１６，１７　フィールド
１８，１９　フィールド
５１，５２，５３，５４，５５，５６，５７，５８，５９，６０，６１　制御線
７０　メモリ
７１　レジスタ
７２　デコーダ
７３，７４　ＡＮＤ回路
７５，７６　フリップフロップ
７７，７８　ＡＮＤ回路
９０　情報線
９１，９２，９３，９４，９５，９６，９７，９８，９９，１００，１０１制御線

【図１】


12
メ　モ　リ
相手番号tn
ｾｷｭﾘﾃｨﾚﾍﾞﾙS1
61
18
フィールド
(tn)
フィールド
(s1)
19
相手番号TN
ｾｷｭﾘﾃｨﾚﾍﾞﾙSL
11
(ｱﾄﾞﾚｽ)
53
(s1)
54
51
レジスタ
52
メモリ制御回路
13
フィールド
(SL)
フィールド
(TN)
16
17
(tn, s1)
55
"1":s1＜SL
警告
(TN, SL)
比較器
60
"1":s1≧SL
"0":s1＜SL
56
14
58
59
57
(TN)
AND
(TN)
15

【図２】


70
メ　モ　リ
参加者番号tn
セキュリティレベルsl
61
18
フィールド (tn)
フィールド (sl)
19
(アドレス) 53
(sl) 54
72
13
メモリ制御回路
91
デコーダ
最低の
セキュリティレベルsm
101
(tn, sl)
55
"1" : sl ≧ SL
"0" : sl < SL
92
93
sm
(TN, SL)
比較器
58
レ　ジ　ス　タ
100
56
14
73
74
AND
AND
95
94
76
F／F
F／F
75
90
97
96
会話，符号化画像
78
AND
AND
77
99
98
71
各参加者へ